**Lindsay Graham**

**Networking**

The first part of this document will outline some of the networking capabilities for the Ubuntu and CentOS servers. It will detail popular commands and provide examples of the output. The second section will include a basic networking script that can be used with each system, and the reasoning for the various commands within the script.

**Ubuntu Server**

To identify what version of Ubuntu is installed, use the **lsb\_release -a** command (Kinsta, 2024). The version is listed on the Description line.

Figure 1.1 Results of **lsb\_release -a**

A screenshot of a computer

Description automatically generated

The **ip addr**, or **ip a**, command displays information about the network interfaces (van Vugt, 2016). The first section indicated by “lo” represents the loopback interface. This interface is used for internal communication within the system. For this server, the IPv4 address is 127.0.0.1. The second section indicated by “enp0s3” represents the broadcast and multicast interface (McKay, 2020). According to McKay, “the “en” stands for ethernet or the wireless adapter, “p0” is the bus number of the ethernet card, and “s3” is the slot number.” The inet, or IPv4 address for this system is 10.0.0.49.

Figure 1.2 Results of **ip addr**

A screenshot of a computer program

Description automatically generated

The **ip route** command shows the interfaces that data packets are sent through. To view the routes that are defined in the Ubuntu server, use the command **ip route**. The first line specifies the default route. In the default route, the “dev enp0s3” specifies that the 10.0.0.1 interface should be used to send packets to the system’s router. The “proto dhcp” signifies that the routing protocol indicated that routes will be selected dynamically. The “metric 100” refers to the preference of one route over another.

Figure 1.3 Results of **ip route**

A screenshot of a computer screen

Description automatically generated

The command to list all installed packages on the Ubuntu server is **apt list –installed** (Gite, 2024). To specifically search for network related packages use the command with grep to search for all packages that start with “net.” The **apt list -–installed** command, used with grep, can search for all network related packages. Below is a list of network related packages that were found with the command **apt list –installed | grep ‘^net.’**

Figure 1.4Results of **apt list –installed | grep ‘^net’**

A screenshot of a computer program

Description automatically generated

This Ubuntu server uses iptables for the firewall. To view the current iptables rules use the command **sudo iptables -L** (Ubuntu, 2020). Figure 1.5 shows that there are no rules in place.

Figure 1.5 Results of **sudo iptables -L**

A screenshot of a computer program

Description automatically generated

The Uncomplicated Firewall (UFW) is an interface that can simply the firewall configuration on the Ubuntu server (Boucheron et al., 2024). The UFW is disabled by default (Ubuntu , 2024).

To check the UFWs status use the command **sudo ufw status**.

Figure 1.6 Results of **sudo ufw status**

A black and white text

Description automatically generated

By default, the UFW’s rules deny incoming traffic and allow outgoing connections. To view which profiles are registered with the UFW, use the command **ufw app list**. The OpenSSH was installed with the server setup, but the Postfix programs were installed with emacs.

Figure 1.7 Results of **sudo ufw app list**

A screenshot of a computer

Description automatically generated

To view the rules that should be run before the command line added rules view the rules.before file in the etc/ufw/ directory.

Figure 1.8 Image of /etc/ufw/before.rules

A screenshot of a computer program

Description automatically generated

To view custom firewall rules use the command **sudo nano /etc/ufw/ufw.conf**.

Figure 1.9 Image of /etc/ufw/ufw.conf

A screenshot of a computer screen

Description automatically generated

The resolv.conf file outlines how the system will resolve alpha-numeric names into numerical network addresses (Debian, 2024). This file will hold the IP addresses of the domain name system (DVS) resolvers, or nameservers, that can do this translation. Below, the IP address 127.0.0.53 is the address used for this purpose.

Figure 1.10 Image of /etc/resolv.conf

A screenshot of a computer screen

Description automatically generated

This server does not have the /etc/network/interfaces configuration file. This is the content of the /etc/network/ directory.

Figure 1.11 Contents of /etc/networks directory

A screenshot of a computer

Description automatically generated

Modern versions of Ubuntu use netplan (Ubuntu Core, 2024). In the /etc/netplan directory, there was a file 50-cloud-init.yaml. This shows the default network configuration.

Figure 1.12 Contents of 50-cloud-init.yaml

A screen shot of a computer

Description automatically generated

To view the ssh server configuration, open the sshd\_config file. This file does not have any rules, only comments (SSH Academy, 2024).

Figure 1.13 results of /etc/ssh/sshd\_config

A screenshot of a computer

Description automatically generated

To explore what types of networking files exist, you can **ls** different network related directories. Here is information about what is in the /etc/network directory.

Figure 1.14 Contents of /etc/network directory

A screen shot of a computer

Description automatically generated

If you find different files, you can use cat to see their contents. Here is the netconfig file.

Figure 1.15 The contents of netconfig

A screenshot of a computer program

Description automatically generated

To see summarized information about system sockets use the **ss** command with the summary option (**-s**). The **-tuln** option shows all the listening TCP and UDP ports.

Figure 1.16 The results of the **ss -s** command

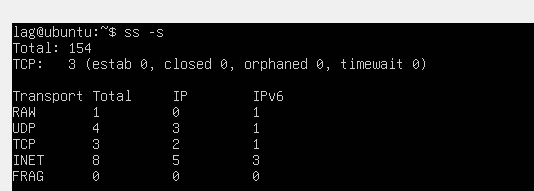


Figure 1.17 The results of **ss -tuln**.

A black screen with white text

Description automatically generated

**CentOS Server**

To identify what version of CentOS is installed, use the **lsb\_release -d** command (Rendek, 2015). The version is listed on the Description line.

Figure 2.1 Results of **lsb\_release -d**

A black background with white text

Description automatically generated

The **ip addr**, or **ip a**, commands display information about the network interfaces (van Vugt, 2016). The first section indicated by “lo” represents the loopback interface. This interface is used for internal communication within the system. For this server, the IPv4 loopback address is 127.0.0.1. The second section indicated by “enp0s3” represents the broadcast and multicast interface (McKay, 2020). According to McKay, “the “en” stands for ethernet or the wireless adapter, “p0” is the bus number of the ethernet card, and “s3” is the slot number.” The inet, or IPv4 address for this system is 10.0.0.155.

Figure 2.2 Results of **ip addr**

A screenshot of a computer

Description automatically generated

The **ip route** command shows the interfaces that data packets are sent through along with which interfaces they should use. To view the routes that are defined in the CentOS server, use the command **ip route**. The first line specifies the default route. In the default route, the “dev enp0s3” specifies that the 10.0.0.1 interface should be used to send packets to the system’s router. The “proto dhcp” signifies that the routing protocol indicated that routes will be selected dynamically. The “metric 100” refers to the preference of one route over another.

Figure 2.3 Results of **ip route**

A screenshot of a computer

Description automatically generated

The command to list all installed packages on the CentOS server is **sudo yum list installed** (Jevtic, 2019). To specifically search for network related packages use the command with grep to search for all packages that start with “net.” The **yum list installed** command, used with grep, can search for all network related packages. Below is a list of network related packages that were found with the command **sudo yum list installed | grep ‘^net.’**

Figure 2.4Results of **sudo yum list installed | grep ‘^net’**

A screenshot of a computer

Description automatically generated

To view the current iptables rules use the command **sudo iptables -L** (Ubuntu, 2020). Figure 1.5 shows that there are no rules in place.

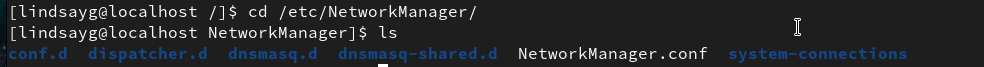
Figure 2.5 Results of **sudo iptables -L**

A screen shot of a computer

Description automatically generated

To view the network configuration settings navigate to etc/NetworkManager/ directory (Horn, 2022).

Figure 2.6 Content of NetworkManager directory



The NetworkingManager.conf file refers to the main configuration file of CentOS. It looks at keyfiles first then ifcfg-rh files next. These files contain the configuration rules.

Figure 2.7 Sample of NetworkManager.conf

A screenshot of a computer program

Description automatically generated

The command **nslookup** with a web address can show the DNS settings for a particular address (Garn, 2022).

Figure 2.8 Results of **nslookup** **www.necc.mass.edu**

A screenshot of a computer

Description automatically generated

To view the ssh server configuration, open the sshd\_config file. This file does not have any rules, only comments (SSH Academy, 2024).

Figure 2.9 results of /etc/ssh/sshd\_config

A screenshot of a computer

Description automatically generated

To see summarized information about system sockets use the **ss** command with the summary option (**-s**). The **-tuln** option shows the listening TCP and UDP ports.

Figure 2.10 The results of the **ss -s** command

A screenshot of a computer

Description automatically generated

Figure 2.11 The results of **ss -tuln**

A computer screen with white text

Description automatically generated

**Network Information Script**

The simple networking script in Figure 3.1 illustrates commonly used network commands. The first two commands, **ip a show enp0s3** and **ip link show enp0s3**, focus on the enp0s3 address and its associated network interface link. The enp0s3 interface is a physical interface, often connected to an ethernet cable or wireless adapter (McKay, 2020). It is the address used to communicate with other network devices and the internet. When using **scp** to transfer files from my laptop to the server, this is the address that I use. If a connectivity issue were to occur, the enp0s3 interface would be helpful for troubleshooting as it is the primary gateway for external communication.

The next command, **ip route show**, provides information about the routing table, which defines where network traffic is forwarded. The results of this command list the routes that are configured on the server. Traffic is routed based on defined rules. If no rule applies, the default route is used. For example, if a new network interface card is installed on a system, a new route may need to be added to enable its use. By reviewing the current routes, administrators can determine if any new routes need to be added, or others removed.

Next, the script retrieves information about the domain name system (DNS) records with the **dig** command. The **dig** command is used to gather details about domain names and their associated records (Dancuk, 2023). In this instance, the script uses **dig www.necc.mass.edu** to query the NECC web address. It also performs a reverse lookup on the server's IP address with the command **dig -x 10.0.0.49**. Network administrators commonly use the **dig** command for troubleshooting DNS issues or verifying DNS configurations.

Lastly, the **ss** command was used to display network statistics, including information about network sockets. The **-s** option with **ss** provides summary statistics, while **-tuln** lists all listening TCP and UDP ports on the system (Wake, 2024). This can be helpful for identifying unexpected listening ports, which might indicate a security risk. The commands were enclosed in brackets to group them together, and their output was appended to a new file named netscript.txt.

Figure 3.1 Simple networking script

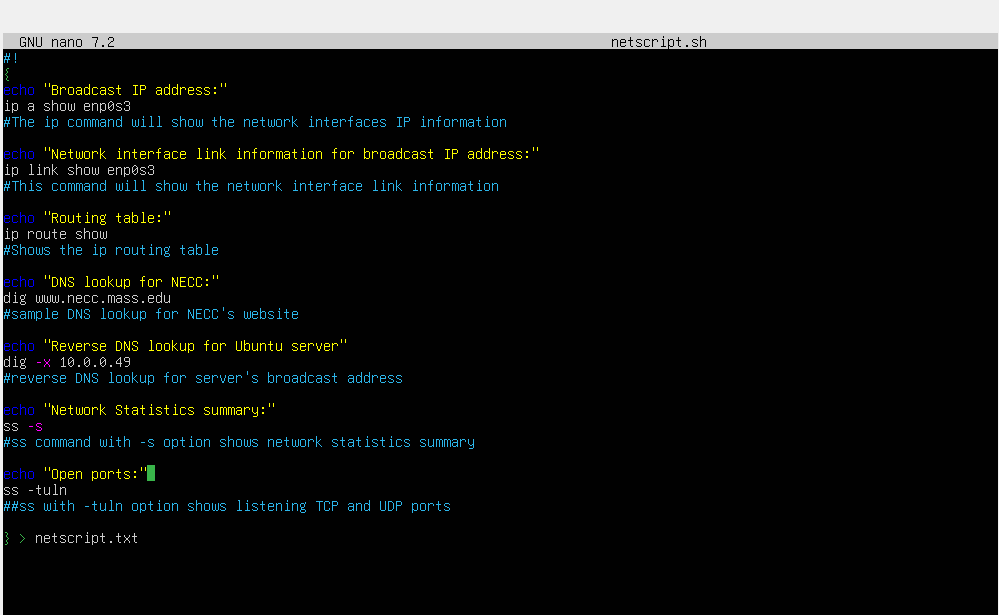


Figure 3.2 Sample of results from cat netscript.txt output file on Ubuntu Server

A screenshot of a computer

Description automatically generated

Figure 3.3 Sample of results from cat netscript.txt on CentOS Server

A screenshot of a computer

Description automatically generated

**References**

Boucheron, B., Camisso, J., & Abid, E. (2024, February 27). *How to Set Up a Firewall with UFW on Ubuntu | DigitalOcean*. Www.digitalocean.com. https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu

Dancuk, M. (2023, September 13). *Linux Network Commands Cheat Sheet | phoenixNAP KB*. Knowledge Base by PhoenixNAP. https://phoenixnap.com/kb/linux-network-commands#ftoc-heading-7

Debian. (2024, August 1). *NetworkConfiguration - Debian Wiki*. Debian.org. https://wiki.debian.org/NetworkConfiguration#Defining\_the\_.28DNS.29\_Nameservers

Garn, D. (2022, April 4). *Linux troubleshooting commands: 4 tools for DNS name resolution problems*. Enable Sysadmin. https://www.redhat.com/sysadmin/DNS-name-resolution-troubleshooting-tools

Gite, V. (2024, August 16). *How do I see what packages are installed on Ubuntu Linux?* NixCraft. https://www.cyberciti.biz/faq/apt-get-list-packages-are-installed-on-ubuntu-linux/

Horn, C. (2022). *RHEL 9 networking: Say goodbye to ifcfg-files, and hello to keyfiles*. Redhat.com. https://www.redhat.com/en/blog/rhel-9-networking-say-goodbye-ifcfg-files-and-hello-keyfiles

Jevtic, G. (2019, April 29). *3 Options to List All Installed Packages in CentOS {Easiest Way}*. Knowledge Base by PhoenixNAP. https://phoenixnap.com/kb/how-to-list-installed-packages-on-centos

Kinsta. (2024, May 7). *How To Check Your Ubuntu Version (Using the Command Line and GUI)*. Kinsta®. https://kinsta.com/knowledgebase/check-ubuntu-version/

McKay, D. (2020, March 4). *How to Use the ip Command on Linux*. How-to Geek. https://www.howtogeek.com/657911/how-to-use-the-ip-command-on-linux/

Rendek, L. (2015, August 4). *How to check CentOS version*. LinuxConfig. https://linuxconfig.org/how-to-check-centos-version

SSH Academy. (2024). *sshd\_config is the OpenSSH server configuration file. How to configure and troubleshoot. Avoid getting accidentally locked out of remote server.* Www.ssh.com. https://www.ssh.com/academy/ssh/sshd\_config

Ubuntu. (2020, April 11). *IptablesHowTo - Community Help Wiki*. Ubuntu.com. https://help.ubuntu.com/community/IptablesHowTo

Ubuntu . (2024). *Firewall*. Ubuntu Server. https://documentation.ubuntu.com/server/how-to/security/firewalls/?\_ga=2.258631562.14676876.1728760528-583595323.1728760528&\_gl=1

Ubuntu Core. (2024). *NetworkManager and netplan*. Ubuntu.com. https://ubuntu.com/core/docs/networkmanager/networkmanager-and-netplan

van Vugt, S. (2016, January 4). *The Linux ip command makes network config easy | TechTarget*. Data Center. https://www.techtarget.com/searchdatacenter/tip/The-Linux-ip-command-makes-network-config-easy

Wake, T. (2024, August 22). *Linux Incident Response - Using ss for Network Analysis | SANS*. Sans.org. https://www.sans.org/blog/linux-incident-response-using-ss-for-network-analysis/